

Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving effect to orders from another Party for expedited production of subscriber information and traffic data

1. BACKGROUND

The Council of Europe [Convention on Cybercrime](#) (also known as the Budapest Convention), which was opened for signature in 2001 and entered into force in 2004, was the first international treaty to focus explicitly on cybercrime and electronic evidence. After 20 years, it remains the most significant one in the area. A large number of countries worldwide, including 26 EU Member States¹, are Parties to the Budapest Convention.



A review of the Budapest Convention is available in the dedicated SIRIUS Quarterly Review [here](#).

In 2003, the Budapest Convention was extended by an [Additional Protocol](#) (First Protocol) covering offences of racist or xenophobic nature.

Following significant developments in the field of information and communication technology which took place since the adoption of the Budapest Convention, on 17 November 2021, after 4 years of negotiations, the Committee of Ministers of the Council of Europe adopted the [Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence](#) (Second Protocol). The Second Protocol was open for signature by the Parties to the Budapest Convention in May 2022 and will enter into force after being ratified by at least five Parties².

The Second Protocol is accompanied by an [Explanatory Report](#) intended to assist Parties in its application. The Budapest Convention itself is similarly accompanied by an [Explanatory Report](#) with the same aim.

The Second Protocol is intended to enhance cooperation among the Parties, as well as between the Parties and service providers and other entities, for obtaining disclosure of electronic evidence for the purpose of criminal investigations or proceedings³.



More information about the Second Protocol is available in the dedicated SIRIUS Quarterly Review [here](#).

An important provision of the Second Protocol aimed at facilitating cooperation between the Parties and private entities is Article 8. Article 8 provides a legal basis for a requesting Party to issue an **order to be submitted as part of a request to another Party** and for the requested Party to have the **ability to give effect to that order by compelling a service provider** in its territory to **produce subscriber information or traffic data** in the service provider's **possession or control**⁴. Article 8 thereby establishes a mechanism that complements the mutual legal assistance provisions set out in the Budapest Convention⁵. It is designed to be more streamlined than mutual legal assistance, as the information the requesting Party must provide is more limited and the process for obtaining the data more rapid⁶.

¹ <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty-num=185>. All EU Member States, except for Ireland.

² Second Protocol, Article 16.

³ Explanatory Report, para. 25.

⁴ Explanatory Report, paras 124, 126.

⁵ Explanatory Report, para. 125.

⁶ Ibid.



The SIRIUS project has received funding from the European Commission's Service for Foreign Policy Instruments (FPI) under contribution agreement No PI/2020/417-500. This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

This document may not necessarily reflect the official position of the Council of Europe or of the Parties to the Budapest Convention on Cybercrime and does not constitute an authoritative interpretation of provisions of this treaty or its protocols.

Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving effect to orders from another Party for expedited production of subscriber information and traffic data



Another important provision of the Second Protocol is Article 7, which - if implemented into the domestic law of the Parties – provides a legal basis for direct cooperation between competent authorities and service providers in the territory of another Party for the purpose of obtaining subscriber information.

Parties may seek enforcement of orders under Article 7 pursuant to Article 8 or another form of mutual assistance⁷. For enforcement via Article 8, the Second Protocol contemplates a simplified procedure of conversion of an order under Article 7 to an order under Article 8⁸.

More information about Article 7 is available in the dedicated SIRIUS Quarterly Review [here](#).

2. SCOPE

• Types of crimes covered

The measure provided for under Article 8 of the Second Protocol is applicable to **specific criminal investigations or proceedings** relating to:

- Criminal offences established in accordance with Section 1 of the Budapest Convention and other criminal offences committed by means of a computer system;
- The collection of evidence in electronic form of a criminal offence; and
- Between Parties to the First Protocol, criminal offences established pursuant to the First Protocol⁹.

Therefore, the specific criminal investigations and proceedings covered include not only cybercrime, but **any criminal offence involving evidence in electronic form**. This means that the measure

provided for under Article 8 of the Second Protocol applies either where a crime is committed by use of a computer system, or where a crime not committed by use of a computer system (for example a murder) involves electronic evidence¹⁰.

This is also confirmed in [Guidance Note #13](#)¹¹, which states that: “The [Cybercrime Convention Committee (T-CY)] agrees that the procedural law provisions and the principles and measures for international co-operation of the [Budapest Convention] are applicable not only to offences related to computer systems and data but also to the collection of electronic evidence of any criminal offence. This broad scope also applies to the measures of the [Second Protocol].”

• Data covered

The measure provided for under Article 8 of the Second Protocol can be used for obtaining **subscriber information and traffic data**. It further only covers **stored and existing data** and does not include any future data or existing data which is in transit.



Parties may **reserve the right not to apply Article 8 to traffic data**¹².

A **Party that reserves the right** not to give effect to orders for traffic data from another Party is **also not permitted to submit orders for traffic data to other Parties** under Article 8(1)¹³.

A list of all declarations and reservations can be found [here](#).

As Article 8 complements, and is therefore without prejudice to, other mutual assistance provisions set out under the Budapest Convention or other multilateral or bilateral agreements, if a requesting

⁷ Second Protocol, Article 7(7).

⁸ Explanatory Report, para. 118.

⁹ Second Protocol, Article 2(1); Budapest Convention, Article 14(2)(a)-(c).

¹⁰ Explanatory Report, para. 33. See also Explanatory Report to the Budapest Convention, paras 141, 243.

¹¹ Although not binding, Guidance Notes adopted by the T-CY represent the common understanding of the Parties regarding

the use of the Budapest Convention and its protocols, see <https://www.coe.int/en/web/cybercrime/guidance-notes>.

¹² Second Protocol, Article 8(13).


¹³ Explanatory Report, para. 147.

Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving effect to orders from another Party for expedited production of subscriber information and traffic data

Party wishes to seek traffic data from a Party that has reserved to that aspect of Article 8, the requesting Party can use another mutual assistance procedure¹⁴.

The term “subscriber information” is defined in Article 18(3) of the Budapest Convention and includes any information held by the administration of a service provider relating to a subscriber to its services (other than traffic data or content data) by means of which can be established:

- The type of communication service used, the technical provisions¹⁵ taken thereto and the period of time during which the person subscribed to the service (Article 18(3)(a));
- The subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, which is available on the basis of the service agreement or arrangement¹⁶ between the subscriber and the service provider (Article 18(3)(b)); or
- Any other information concerning the site or location where the communication equipment is installed, which is available on the basis of the service agreement or arrangement (Article 18(3)(c)).

 It is notable that **the definition of “subscriber information”, as per Article 18(3) of the Budapest Convention, may also include information that under EU law is considered as traffic data.**

The term “traffic data” is defined in Article 1(d) of the Budapest Convention and includes any

computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

Where different types of data (subscriber information, traffic data and content data) are sought at the same time, it may be **more efficient to seek all three forms of data** for the same account **via a single traditional mutual assistance request**, rather than to seek some types of data via the measure provided by Article 8 and others via a separate mutual assistance request¹⁷.

• Entities covered

Article 8 of the Second Protocol applies to “**service providers**”. The term “service provider” is broadly defined in Article 1(c) of the Budapest Convention and includes:

- Any public or private entity that provides to users of its service **the ability to communicate** by means of a computer system; and
- Any other entity that **processes or stores computer data** on behalf of such communication service or users of such service.

This definition covers both providers of electronic communication services and of internet society services¹⁸.

¹⁴ Explanatory Report, para. 125.

¹⁵ The term “technical provisions” includes all measures taken to enable a subscriber to enjoy the communication service, including the reservation of a technical number or address (for example, telephone number, website address / domain name, e-mail address) and the provision and registration of communication equipment used by the subscriber (for example, telephone devices, call centres, LANs). See Explanatory Report to the Budapest Convention, para. 179.

¹⁶ The reference to a “service agreement or arrangement” includes any kind of relationship on the basis of which a client uses the service provider’s services. See Explanatory Report to the Budapest Convention, para. 183.

¹⁷ Explanatory Report, para. 125.

¹⁸ [Guidance Note #10](#), p. 5, footnote 6.

Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving effect to orders from another Party for expedited production of subscriber information and traffic data



It is notable that the definition of “service provider” included in the EU Electronic Evidence legislative package ([Electronic Evidence Regulation](#) and [Electronic Evidence Directive](#)), which will apply as of 2026¹⁹, is broader than the one set out in the Budapest Convention and includes both service providers as defined in Article 1(c) of the Budapest Convention, as well as entities providing domain name registration services, as referred to under Article 6 of the Second Protocol²⁰.

Furthermore, the EU [Digital Services Act](#) (DSA) applies to providers of “intermediary services”, known as certain information society services which qualify as “mere conduit”, “caching” and “hosting” services²¹. In the field of direct cooperation between authorities and providers of intermediary services active on EU territory, the DSA recognises the potentially overlapping scope of application of the EU Electronic Evidence legislative package. Similarly, providers of intermediary services falling within the scope of the DSA would also fall under the definition of service providers as set out in the Budapest Convention.

3. DEFINING THE TOOLBOX

When implemented into the domestic laws of the Parties, Article 8 of the Second Protocol will provide a basis for a **competent authority** in a requesting Party to **issue an order to be submitted as part of a request to another Party** for the purpose of **compelling a service provider in the requested**

Party’s territory to produce specified and stored subscriber information and traffic data in that service provider’s possession or control.

The term “**service provider in the territory of another Party**” requires that the service provider is **physically present** in the other Party. The mere fact that, for example, a service provider has established a contractual relationship with a company in a Party, but the service provider itself is not physically present in that Party, would not constitute the service provider being “in the territory” of that Party²².

The term “**possession or control**” refers to **physical possession**, as well as to situations where the data is not in the service provider’s physical possession but instead **stored remotely but under the service provider’s control**.

4. CONDITIONS AND SAFEGUARDS

A – OVERALL SYSTEM OF SAFEGUARDS

- **Purpose limitation**

In addition to what is noted above (see section [Scope](#), in particular the sections on types of crimes covered and data covered), orders under Article 8 may only be issued and submitted in the context of “specific investigations or proceedings”, for information that is “needed for” that investigation or proceeding²³.

¹⁹ The [Electronic Evidence Regulation](#) and the [Electronic Evidence Directive](#) were published in the Official Journal of the European Union on 27 July 2023. The Regulation shall apply from 18 August 2026 while in the case of the Directive, EU Member States shall adopt the necessary measures to comply with it by 18 February 2026.

²⁰ The EU Electronic Evidence legislative package defines a “service provider” as any natural or legal person that provides electronic communication services; internet domain name and IP numbering services such as IP address assignment, domain name registry, domain name registrar and domain name-related privacy and proxy services; and any other information society service that provides the ability to its users to communicate with each other or makes it possible to store or otherwise process data on behalf of the users to whom the service is provided, provided that the storage of data is a defining component of the service provided to the user (Electronic Evidence Regulation, Article 3(3); Electronic Evidence Directive, Article 2(1)).

²¹ In accordance with Article 3(g) of the DSA, “intermediary service” means one of the following information society services: (i) a “mere conduit” service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network; (ii) a “caching” service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information’s onward transmission to other recipients upon their request; (iii) a “hosting” service, consisting of the storage of information provided by, and at the request of, a recipient of the service.

²² Explanatory Report, para. 128.

²³ Second Protocol, Articles 2, 8(1).

Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving effect to orders from another Party for expedited production of subscriber information and traffic data

- **Additional safeguards**

Article 8(3), specifying the requirements for orders under Article 8 and the supporting information to be provided by the requesting Party (see section [Requirements for orders under Article 8](#)), may assist in applying domestic safeguards²⁴. Additionally, as noted above, Parties may reserve the right not to apply Article 8 to traffic data²⁵.

B – ARTICLE 13 OF THE SECOND PROTOCOL: CONDITIONS AND SAFEGUARDS

- **Protection of human rights**

Article 13 of the Second Protocol makes a specific reference to Article 15 of the Budapest Convention and requires Parties to ensure that the powers and procedures established under the Second Protocol – thus including the measure provided for under Article 8 – are subject to an appropriate level of protection for human rights and liberties under their domestic law. These include standards or minimum safeguards arising pursuant to a Party's obligations under applicable international human rights instruments²⁶.

- **Principle of proportionality**

Article 15(1) of the Budapest Convention also requires Parties to apply the principle of proportionality. This will be done in accordance with each Party's relevant domestic law principles. In the case of European countries, these principles will be derived from the European Convention on Human Rights (ECHR) and related jurisprudence, meaning that the powers of competent authorities must be **proportional to the nature and**

circumstances of the offence²⁷. Other Parties may apply related domestic law principles, such as principles of **relevance** (i.e. the evidence sought must be relevant to the investigation or prosecution), **limitations on overly broad orders**²⁸ or **exclude their application in cases concerning minor crimes**²⁹.

- **Other conditions and safeguards**

Pursuant to Article 15(2) of the Budapest Convention, applicable conditions and safeguards include, as appropriate, judicial or other independent supervision, grounds justifying the application of the power or procedure and the limitation on the scope or the duration thereof. Other safeguards that must be addressed under domestic law include: the right against self-incrimination, legal privileges, and specificity of individuals or entities subject to the measure³⁰.

- **Public interest, sound administration of justice and rights of third parties**

In accordance with Article 15(3) of the Budapest Convention, when implementing the provisions of Article 8, Parties shall first consider the sound administration of justice and other public interests (for example public safety, public health, the interests of victims, respect for private life). To the extent that it is consistent with these interests, consideration shall also be given to the impact of the measure on the rights, responsibilities and legitimate interests of third parties, which may include, for example, protection from liability for disclosure³¹.

²⁴ Explanatory Report, para. 219.

²⁵ Second Protocol, Article 8(13).

²⁶ These instruments include the [1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms](#) (ECHR) and its additional protocols (in respect of European states that are parties to them), other applicable human rights instruments, such as e.g. the [1969 American Convention on Human Rights](#) and the [1981 African Charter on Human Rights and Peoples' Rights](#) (in respect of states in other regions of the world which are parties to them)

and the [1966 International Covenant on Civil and Political Rights](#) (Explanatory Report to the Budapest Convention, para. 145).

²⁷ Explanatory Report, para. 97; Explanatory Report to the Budapest Convention, para. 146.

²⁸ Explanatory Report, para. 97; Explanatory Report to the Budapest Convention, para. 145.

²⁹ Explanatory Report to the Budapest Convention, paras 146, 174.

³⁰ Explanatory Report to the Budapest Convention, para. 147.

³¹ Explanatory Report to the Budapest Convention, para. 148.

Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving effect to orders from another Party for expedited production of subscriber information and traffic data

C – ARTICLE 14 OF THE SECOND PROTOCOL: PROTECTION OF PERSONAL DATA

Article 14 of the Second Protocol provides in its paragraphs 2 to 15 a robust system for data protection. This includes safeguards regarding purpose and use of the data; data quality and integrity; sensitive data; retention of data; automated decision-making; security; records and logging; transparency and notice regarding processing, retention periods, data disclosure, access rectification and redress available; right to access and rectification; judicial and non-judicial remedies; and independent oversight³². A Party may also suspend the transfer of personal data to another Party based on substantial evidence of systematic or material breach of Article 14³³.

Pursuant to Article 14(1)(a), each Party shall process personal data that it receives under the Second Protocol in accordance with the specific safeguards set out in Article 14(2)-(15), with two exceptions:

- If, at the time of transfer of data, both the transferring Party and the receiving Party are bound by an international agreement establishing a comprehensive framework between those Parties for the protection of personal data, which is applicable to the transfer of personal data for the purpose of the prevention, detection, investigation and prosecution of criminal offences (Article 14(1)(b)). This would include, for example, [Convention 108+](#) and the [EU-US Umbrella Agreement](#)³⁴.
- If the transferring Party and the receiving Party, not bound by an international agreement as described above, nevertheless agree that the transfer of

data under the Second Protocol may take place on the basis of other agreements or arrangements between them in lieu of Article 14(2)-(15). For EU Member States, in relation to transfers of personal data to third countries, such an alternative agreement would have to comply with the requirements of EU data protection legislation.

5. REQUESTING PARTY

A – ISSUING AUTHORITIES

Orders under Article 8 of the Second Protocol must be issued by competent authorities³⁵.

The Second Protocol defines the term “competent authority” as a judicial, administrative or other law enforcement authority that is **empowered by domestic law to order, authorise or undertake the execution of measures under the Second Protocol for the purpose of collection or production of evidence** with respect to specific criminal investigations or proceedings³⁶.

The domestic legal system of a Party will govern which authority is considered as a competent authority to issue an order under Article 8 of the Second Protocol.



The **authorities competent to issue an order** in accordance with Article 8(1) may **not necessarily be the same** as the **authorities designated to submit the order to be given effect** in accordance with Article 8(10)(a)³⁷.

B – ISSUING PROCEDURE

Orders under Article 8 of the Second Protocol are initiated by the competent authority of one Party and submitted as part of a request to another Party. The issuing process is outlined in the domestic law

³² For more information, see Second Protocol, Article 14(2)-(14) and Explanatory Report, paras 227-281.

³³ Second Protocol, Article 14(15).

³⁴ Explanatory Report, para. 222.

³⁵ Second Protocol, Article 8(1).

³⁶ Second Protocol, Article 3(2)(b).

³⁷ Explanatory Report, para. 127.

Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving effect to orders from another Party for expedited production of subscriber information and traffic data

of the Party issuing the order and remains subject to legal safeguards (see also section [Conditions and safeguards](#)).

The term “order” encompasses any legal process designed to compel a service provider to provide subscriber information or traffic data such as a production order, a subpoena, or any other legally sanctioned mechanism³⁸.

REQUIREMENTS FOR ORDERS UNDER ARTICLE 8

Pursuant to Article 8(3)(a), the order must specify:

- The **issuing authority** and the **date** of issuance (Article 8(3)(a)(i));
- A statement that the order is **submitted pursuant to the Second Protocol** (Article 8(3)(a)(ii));
- The **name and address of the service provider(s)** to be served (Article 8(3)(a)(iii));
- The **offence(s)** that is / are the subject of the criminal investigation or proceeding (Article 8(3)(a)(iv));
- The **authority seeking the information or data**, if not the issuing authority, such as e.g. where an investigating or prosecuting authority is seeking the data while a judge issues the order³⁹ (Article 8(3)(a)(v)); and
- A detailed **description of the specific information or data** sought (Article 8(3)(a)(vi)).

Pursuant to Article 8(3)(b), supporting information shall specify:

- The **domestic legal grounds** that **empower the authority to issue the order** (Article 8(3)(b)(i));
- The **legal provisions** and **applicable penalties for the offence(s)** being

investigated or prosecuted (Article 8(3)(b)(ii));

- The reason **why the requesting Party believes** that the **service provider** is in **possession or control of the data** (Article 8(3)(b)(iii));
- A **summary of the facts** related to the investigation or proceeding (Article 8(3)(b)(iv));
- The **relevance of the information or data** to the **investigation or proceeding** (Article 8(3)(b)(v));
- **Contact information** of an authority or authorities that **may provide further information** (Article 8(3)(b)(vi));
- Whether **preservation** of the information or data has **already been sought**, including the **date of preservation** and any applicable **reference number** (Article 8(3)(b)(vii); this information may permit the requested Party to match the request to a previous preservation request and thereby facilitate disclosing the information or data originally preserved⁴⁰; and
- Whether the **information or data** has already been **sought by other means**, and, if so, in what manner (Article 8(3)(b)(viii); this mainly addresses whether the requesting Party has already sought subscriber information or traffic data directly from the service provider⁴¹.

The supporting information is to be provided for the purposes of assisting the requested Party to give effect to the order and **shall not be disclosed to the service provider without the consent of the requesting Party**. In particular, the summary of the facts and the statement regarding the relevance of the information or data to the investigation or proceeding is provided to the requested Party for

³⁸ Explanatory Report, para. 126.

³⁹ Explanatory Report, para. 132.

⁴⁰ Explanatory Report, para. 133.

⁴¹ Ibid.

Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving effect to orders from another Party for expedited production of subscriber information and traffic data

the purpose of determining whether there is a ground for imposing terms or conditions or for refusal (see section [Requested Party](#)), but is often subject to the secrecy of the investigation⁴². At the time of making a request, Parties should **indicate if there is any information under Article 8(3)(b) that may be shared with the service provider**⁴³.



A Party **may declare** that **additional supporting information is required** to give effect to orders under Article 8⁴⁴. When making such a declaration, Parties should be **as specific as possible** with regard to the type of information required⁴⁵.

For example, under some Parties' domestic law, the production of traffic data may require further information because there are additional requirements in their laws for obtaining such data. Others may require additional information where the order was not issued or reviewed by a prosecutor or another judicial or independent administrative authority of the requesting Party⁴⁶.

Pursuant to Article 8(3)(c), the requesting Party may also request that the requested Party carry out **special procedural instructions**. This may include, for example, non-disclosure of the order to the subscriber or authentication forms to be completed for the evidence to be provided⁴⁷. Any such requirements should be indicated at the outset, as they may require additional processes within the requested Party⁴⁸.

If the requested Party **cannot comply with any special procedural instructions** under Article 8(3)(c) in the manner requested (for example, where the procedural instructions are not available under the requested Party's law), it shall **promptly inform the**

requesting Party, and, if applicable, specify any conditions under which it could comply. This will give the **requesting Party** the opportunity to **determine whether** or not it wishes to **continue with the request**⁴⁹.

The requested Party may also require additional information from the requesting Party in order to support any applications for supplementary orders, such as confidentiality orders (non-disclosure orders)⁵⁰.

Lastly, pursuant to Article 4(1) of the Second Protocol, orders under Article 8 and any accompanying information shall be in a **language acceptable to the requested Party** or be **accompanied by a translation** into such a language.

TRANSMISSION OF ORDERS UNDER ARTICLE 8

As regards the authorities who may transmit orders under Article 8 as part of a request to another Party, a Party may declare that it requires that **requests** by other Parties be **submitted by the central authority of the requesting Party** or by such **other authority as mutually determined** between the Parties concerned⁵¹. Parties are encouraged to provide as much flexibility as possible for the submission of requests⁵².

A Party shall communicate to the Secretary General of the Council of Europe and keep up to date the **contact information of the authorities designated to submit and receive orders** under Article 8⁵³.

An updated **register of the authorities so designated** by the Parties shall be set up and kept updated by the Secretary General of the Council of Europe⁵⁴. This

⁴² Explanatory Report, para. 134.

⁴³ Explanatory Report, para. 131.

⁴⁴ Second Protocol, Article 8(4).

⁴⁵ Explanatory Report, para. 137.

⁴⁶ Ibid.

⁴⁷ Explanatory Report, paras 131, 135.

⁴⁸ Explanatory Report, para. 135.

⁴⁹ Explanatory Report, para. 140.

⁵⁰ Ibid.

⁵¹ Second Protocol, Article 8(11).

⁵² Explanatory Report, para. 145.

⁵³ Second Protocol, Article 8(1)(a)-(b). Parties need not give the name and address of a specific individual but may identify an office or unit that has been deemed competent for the purposes of sending and receiving orders under Article 8 (Explanatory Report, para. 144.).

⁵⁴ Second Protocol, Article 8(12).

Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving effect to orders from another Party for expedited production of subscriber information and traffic data

information can assist requested Parties to verify the authenticity of requests⁵⁵.

Pursuant to Article 8(5), the requested Party shall accept requests in electronic form. Accordingly, a Party may transmit an order under Article 8 as part of a request in electronic form, for example by using e-mail, electronic portals or other means. However, there is no requirement that only this format may be used. Furthermore, appropriate levels of security and authentication may be required.

5. REQUESTED PARTY

A – EXECUTION OF THE REQUEST

Pursuant to Article 8(2), Parties are required to **give effect to orders** submitted under Article 8(1) **from another Party**. This means that the requested Party must be able to **compel the service provider to provide the subscriber information and traffic data** sought using the mechanism of its choice, provided that the mechanism makes the order enforceable under the requested Party's domestic law and meets the requirements of Article 8. For example, a Party may give effect to an order under Article 8 by accepting it as equivalent to domestic orders, by endorsing it to give it the same effect as a domestic order or by issuing its own production order. As any such mechanism will be subject to the terms of the law of the requested Party, the requested Party can ensure that its own law, including constitutional and human rights requirements, is satisfied, especially in relation to any additional safeguards including those necessary for the production of traffic data⁵⁶.

The requested Party must moreover take reasonable steps to proceed expeditiously with respect to the request. It shall make **reasonable efforts** to process requests and have the **service provider served within 45 days** after receipt of all

the necessary documents and information. It shall also **order the service provider to produce the subscriber information within 20 days and traffic data within 45 days**⁵⁷.

To facilitate the production of the information or data, the requested Party may communicate to the service provider additional information, such as the **method of production and to whom the data should be produced** in the requested Party⁵⁸.

Following production of the information or data by the service provider, the requested Party shall provide for its **transmission to the requesting Party without undue delay**⁵⁹.

There are many factors that may delay production of the data or information, such as service providers objecting, not responding to requests or not meeting the return date for production, as well as the volume of requests a requested Party may be asked to process. Therefore, requested Parties are required to make **reasonable efforts to complete only the processes under their control**⁶⁰ (i.e. make reasonable efforts to process the request in a timely manner and have the service provider served within 45 days after receipt of all the necessary documentation, order the service provider to produce the data within the time limits set out in the Second Protocol and transmit the data to the requesting Party without undue delay following its production by the service provider).

B – LIMITATION ON USE

Pursuant to Article 8(8) of the Second Protocol and Article 28(2)(b) of the Budapest Convention, the requested Party may make the supply of information or material in response to a request dependent on the condition that it is not used for investigations or proceedings other than those stated in the request.

⁵⁵ Explanatory Report, para. 146.

⁵⁶ Explanatory Report, para. 129.

⁵⁷ Second Protocol, Article 8(6)(a)(i)-(ii); Explanatory Report, para. 139.

⁵⁸ Explanatory Report, para. 136.

⁵⁹ Second Protocol, Article 8(6)(b).

⁶⁰ Explanatory Report, para. 139.

Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving effect to orders from another Party for expedited production of subscriber information and traffic data

C – REFUSAL TO EXECUTE A REQUEST

Pursuant to Article 8(8), the requested Party may **refuse to execute a request** on the grounds set out in Article 25(4) or Article 27(4) of the Budapest Convention. It shall **notify** the requesting Party **as soon as possible** of such refusal.



Article 25(4) of the Budapest Convention refers to **grounds for refusal set out in any applicable mutual assistance** treaties and in domestic law.

Article 27(4) of the Budapest Convention allows for refusal where:

- The request concerns an offence which the requested Party considers a **political offence** or an offence **connected with a political offence**; or
- The execution of the request is likely to prejudice its **sovereignty, ordre public** or other **essential interests**.

In order to promote the principle of providing the widest measure of co-operation⁶¹, **grounds for refusal** established by a requested Party should be **narrow** and **exercised with restraint**, in line with the objectives to eliminate barriers to transborder sharing of subscriber information and traffic data, and to provide more efficient and expedited procedures than traditional mutual assistance⁶².

D – IMPOSITION OF CONDITIONS AND POSTPONEMENT OF EXECUTION OF A REQUEST

Pursuant to Article 8(8), the requested Party may also **impose conditions** it considers necessary to permit the execution of the request⁶³, such as confidentiality⁶⁴, or **postpone the execution** of a request for the reasons set out in Article 27(5) of the Budapest Convention, i.e. where the execution of the request would prejudice criminal investigations or proceedings conducted by its authorities⁶⁵.

The requested Party shall **notify** the requesting Party **as soon as practicable** of the conditions or postponement⁶⁶. It shall also notify the requesting Party of any other circumstances that are likely to significantly delay the execution of the request⁶⁷.

If the **requesting Party cannot comply with a condition imposed** by the requested Party under Article 8(8), it shall promptly inform the requested Party, who shall then determine whether the information or material should nevertheless be provided⁶⁸.

If the **requesting Party accepts the condition**, it shall be **bound by it**. The requested Party that supplies information or material subject to such a condition may require the requesting Party to explain in relation to that condition the use made of such information or material⁶⁹.

⁶¹ Second Protocol, Article 5(1).

⁶² Explanatory Report, para. 142.

⁶³ Second Protocol, Article 8(8).

⁶⁴ Explanatory Report, para. 141.

⁶⁵ Second Protocol, Article 8(8).

⁶⁶ Ibid.

⁶⁷ Ibid.

⁶⁸ Second Protocol, Article 8(9)(a).

⁶⁹ Second Protocol, Article 8(9)(b).